

## UNITED STATES DISTRICT COURT

for the  
Southern District of Illinois

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)

Premises located at 143 CoffeeTree Lane, Makanda, IL  
62958-2736

Case No. 20-mj-8193-GCS

## SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Southern District of Illinois  
(identify the person or describe the property to be searched and give its location):

See Attachment A - description of the property to be searched and its location.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B - description of property to be seized.

**YOU ARE COMMANDED** to execute this warrant on or before December 13, 2020 (not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Magistrate Judge Gilbert C. Sison  
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for        days (not to exceed 30) ☐ until, the facts justifying, the later specific date of       

Date and time issued: 11/30/2020 at 2:16pm

Gilbert C. Sison  
Judge's signature

City and state: East Saint Louis, Illinois

Magistrate Judge Gilbert C. Sison

Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

**Return**

Case No.:

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

**Certification**

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: \_\_\_\_\_

\_\_\_\_\_  
*Executing officer's signature*\_\_\_\_\_  
*Printed name and title*

**ATTACHMENT A**

The property to be searched is located at 143 CoffeeTree Lane, Makanda, Jackson, County, Illinois 62958-2736, which is a two-story residence, brick façade, siding around the residence, with two garage door, single family home.



**ATTACHMENT B**

**I. Information to be seized by Law Enforcement Personnel at the location described in Attachment A, to include all outbuildings, structures, and conveyances located upon the property described in Attachment A.**

All information that constitutes evidence and instrumentalities concerning violations of property of Title 18, United States Code, Section 1001 (Statements or entries generally), and Title 18, United States Code, Section 1343 (Fraud by Wire).

A. Electronic files, computer executable programs, email messages, electronic communications, attachments, and any other electronic files that contain information located on any computer or storage medium located at the target address which have a connection to:

1. Applications, proposals, and/or contracts associated with obtaining a research grant or employment from the National Science Foundation and other federal agencies of the United States and/or from the People's Republic of China, including the Natural Science Foundation of Guangdong Province, National Natural Science Foundation of China, National Science Foundation of China, University of Electronic Science and Technology of China, Guangdong University of Technology, Foshan University, Shenzhen University, and other affiliated entities yet to be identified (collectively, "People's Republic of China").
2. Communication related to obtaining a grant or contract for employment from the United States and/or the People's Republic of China.
3. Communications, records, information, or documents related to fulfilling employment contract stipulations for the People's Republic of China.
4. Records or information about payments or other funds connected to grants or employment from the United States and/or People's Republic of China.

5. Records or information indicating the true nature of MingQing Xiao travel to the People's Republic of China.

6. Record or information supporting a scheme to defraud the United States, while being employed and conducting research for the People's Republic of China.

7. Any other indicia relating to the wire fraud or false official statements.

B. Paper files and file storage containers (including locked) located at this address that contain evidence of:

1. Applications, proposals, and/or contracts associated with obtaining a research grant or employment from the National Science Foundation and other federal agencies of the United States and/or from the People's Republic of China, including the Natural Science Foundation of Guangdong Province, National Natural Science Foundation of China, National Science Foundation of China, University of Electronic Science and Technology of China, Guangdong University of Technology, Foshan University, Shenzhen University, and other affiliated entities yet to be identified (collectively, "People's Republic of China"). Communication related to obtaining applications, proposals, or contracts to obtain a grant or employment from the United States and/or the People's Republic of China.

2. Communications, records, information, or documents related to fulfilling employment contract stipulations with the People's Republic of China;

3. Records or information about payments or other funds connected to from grants or employment from the United States and/or People's Republic of China;

4. Records or information indicating the true nature of MingQing Xiao's travel to the People's Republic of China;
5. Records or information supporting a scheme to defraud the United States, while being employed and conducting research in the People's Republic of China.
6. Any other indicia relating to the wire fraud or false official statements.

C. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant:

1. Evidence of who used, owned, or controlled the computer or storage medium at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
2. Evidence of software that would allow others to control or track the computer or storage medium, such as viruses, cookies, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
3. Evidence of the lack of such malicious software;
4. Evidence indicating how and when the computer or storage medium was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

5. Evidence indicating the computer user's state of mind as it relates to the crime under investigation; evidence of the attachment to the computer or storage medium of other storage devices or similar containers for electronic evidence;
6. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the computer or storage medium;
7. Evidence of the times the computer or storage medium was used;
8. Passwords, encryption keys, and other access devices that may be necessary to access the computer or storage medium;
9. Documentation and manuals that may be necessary to access the computer or storage medium or to conduct a forensic examination of the computer or storage medium;
10. Records of or information about Internet Protocol addresses used by the computer or storage medium;
11. Records of or information about the computer or storage medium's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
12. Contextual information necessary to understand the evidence described in this attachment.

**D. Definitions:**

1. As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as

writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

2. The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

3. The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

E. This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.